THE CERTIFICATION OF THE INTERIM KEY ESCROW SYSTEM

Ellen Flahavin & Ray Snouffer
National Institute of Standards and Technology
Building 820, Room 414
Gaithersburg, MD 20899
(301) 975-3871 & (301) 975-4436
flahavin@csmes.ncsl.nist.gov
ray.snouffer@nist.gov

1. INTRODUCTION

The U.S. Government Key Escrow System (KES) provides for lawfully authorized access to the key required to decipher communications secured with products built in conformance with the Escrowed Encryption Standard, Federal Information Processing Standards Publication (FIPS) 185. This paper is intended for presentation at the 1996 National Information Systems Security Conference. The objective of this paper is to describe the certification and accreditation of the Interim KES and provide a historical overview of the Key Escrow Certification Working Group's (KECWG) activities. The defined purpose of the certification working group is to perform a certification on both the interim and the final KES in accordance with the Guideline for Computer Security Certification and Accreditation (FIPS 102). FIPS 102 provides guidelines for computer security certification and accreditation of sensitive computer security applications. The National Institute of Standards and Technology (NIST) chairs the KECWG. In addition to NIST, the membership consists of the Department of Justice (DOJ), the Department of Treasury, the Federal Bureau of Investigation (FBI), the National Security Agency (NSA) and the Department of Commerce (DOC).

1.1 The National Key Escrow Program

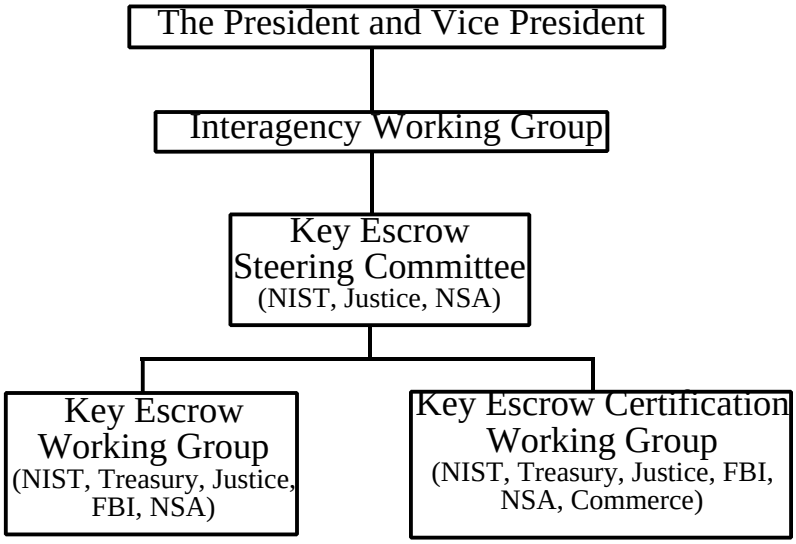
The Key Escrow System was developed to support of the U.S. Government's Escrow Encryption Standard (FIPS-185) and Presidential Decision Directive/NSC-5. The primary objective of this program is to provide the U.S. Government and the private sector with high-quality, secure communications products without jeopardizing effective law enforcement, public safety, and national security. The initiative is based on a special tamper-resistant hardware encryption device (Clipper/Capstone Chip) and a KES. The KES is an interagency program, with support from NIST, DOJ, Treasury, FBI, and NSA. NIST serves as the National Program Manager for Key Escrow; overseeing the current Interim System and the development of the Final System.

1.2 Roles, Responsibilities and Organization of the Participating Agencies

Each agency participating in the KES provides unique support to the program. NIST serves two distinct roles, that of Program Manager and one of the two Escrow Agents. Treasury serves as the second Escrow Agent. The Department of Justice acts as the System Security Manager, system accreditor, and one of the two Family Key Agents. The FBI serves as the second Family

Key Agent and as the initial Law Enforcement Agent. The National Security Agency is responsible for system development and system engineering support.

The overall program is supported through a system of working groups and committees. The Vice President of the United States heads the organizational structure. The Inter-agency Working Group (IWG) provides senior level support to the Vice President on technology and policy. The KES Steering Committee was established to provide the participating agencies with a senior level forum for discussing and resolving issues arising from the interagency nature of the program. Overall KES policy and budget issues are also the responsibilities of the Steering Committee. Further support for the program is provided by the Key Escrow System Working Group (KESWG) and the KECWG. Additional information on the KESWG and the KECWG and their role in system certification are provide in sections 1.4 and 1.5. The following diagram shows the structure of the KES Program.



1.3 Basis For Establishment of the KES Certification Working Group

The KES helps to ensure that the unique keys and key components are released only for legally authorized surveillance activities and only for the duration of the authorization period. At its June 3, 1994 meeting, the KES Steering Committee agreed that the KES would be certified by a committee consisting of representatives from appropriate government agencies and accredited by DOJ. The National Program Manger for Key Escrow established the KECWG to certify both the interim and the final KES. The KES certification will be used as input to the corresponding DOJ accreditation.

1.4 Scope of the C&A Effort

Certification is required by Circular A-130 of the Office of Management and Budget (OMB), for

all computer applications processing Sensitive Unclassified (hereafter referred to as Sensitive) information. FIPS PUB 102, Guideline to Computer Security Certification and Accreditation, 27 September 1983, and the NSA Draft C&A Process Handbook were used to define the certification methodology employed. FIPS PUB 102 presents, in detail, an approach to developing a certification and accreditation program. The NSA Draft C&A Handbook provides a technical process for certifying applications. The activities of the KECWG include the following:

Writing the Certification, Security, and System Test and Evaluation Plans,
Implementing the certification process,
Other tasks specified in FIPS 102 that the KECWG believes necessary for certification,
Evaluating the Risk Assessment and developing a Statement of Residual Risk, and
Providing a recommendation and a certification package to the KES Accreditor.

1.5 The Key Escrow System Working Group

The KESWG was established concurrently with the KECWG by the National Program Manager for Key Escrow. However, The KECWG is an independent group and does not receive direction from the KESWG. The purpose of the KESWG is to manage the development and operation of the KES under the guidance of the Key Escrow Steering Committee. The National Program Manager for Key Escrow reports the activities of the KESWG to the Steering Committee. The activities of the KESWG include the following:

Developing the KES, including subsystems and documentation,
Operating the KES,
Baselining documentation for hardware, software, and operational procedures,
Establishing and maintaining the KES Configuration Management Process,
Planning and implementing improvements to the KES, and
Establishing operational agreements between its members.

Additionally, the KESWG is responsible for developing documents which are essential to system certification. These include the KES Security Policy and the KES Protocols and Procedures (P&P). All system certification testing for the Interim KES is based on the KES P&P document. The KES Security Policy serves as the basis for the KES Security Plan.

2.0 SECURITY ENGINEERING

Security engineering (including C&A) for KES was included as part of the system engineering life cycle. The security engineering tasks were developed and executed concurrently with the system design and development activities. These activities included: developing a security architecture, defining security requirements, and preparing a System Security Plan (SSP).

2.1 Define Security Requirements

The KESWG along with the NSA system developer agreed on a set of security requirements and

identified implementation issues. To ensure compliance with the requirements, reviews were held between the KESWG and the NSA system developer. The system developer is responsible for defining requirements, developing the KES architecture (specifications), as well as designing, implementing and testing the KES. The KECWG is also responsible for testing the system. At the completion of the requirements definition process, the security requirements were included with the functional requirements in the KES Security Policy. This document was reviewed and approved by the KESWG.

2.2 The C&A Process

Certification of the KES involved a technical assessment of the security functions to determine the extent that these functions met the KES security requirements and the KES Security Policy. This certification also included executing security tests to demonstrate the adequacy of the security features and requirements. The test results were included in the certification package for review by the system accreditor. Accreditation is a management decision by DOJ which is required prior to declaring the KES operational.

FIPS PUB 102, Guideline for Computer Security Certification and Accreditation, was used to develop the KES C&A Process. This standard was used because the KES is authorized and staffed by federal agencies; and is used for the processing of sensitive information. NIST is responsible for providing guidance to agencies that process sensitive information. As defined in FIPS PUB 102, the certification effort is divided into basic and detailed evaluations. Detailed evaluation focuses on whether or not specific security features operate correctly.

The NSA draft C&A Handbook was used to further define the KES C&A process. The handbook was used by the KECWG to tailor the certification efforts to the particular purpose, environment, degrees of assurance, and criticality of the system as well as threats to the system.

Phase One C&A focused on existing physical and administrative/personnel security because of the limited number of implemented technical security features. The goals of this phase were to test the KES Protocols and Procedures (P&P), evaluate the certification process itself, and make refinements to the process prior to beginning Phase Two C&A. Since the interim system is primarily manual, the testing was performed sequentially.

2.3 Functional Certification Tasks

Step 1 - Identify the System

The purpose of this step was to identify system specific information that would impact the certification effort. This information included identifying the Accreditor, committing resources by management, establishing the system boundary, and determining the certification type. The determination of the certification type included looking at key aspects of the system such as assurance, confidentiality, integrity, authenticity, and availability. This determination indicated that a type 3 moderate certification as specified in the C&A Handbook, was required. This type of certification is more detailed and complex and is generally used for systems that require higher

degrees of assurance, have a greater level of risk, and are more complex.

Step 2 - Planning

The second step was to develop a certification plan. This plan consisted of determining the composition of the certification team, incorporating milestones, obtaining necessary resources, and documenting planning information.

Step 3 - Perform System Analysis

A comprehensive analysis of both the technical and non-technical security features and other safeguards of the system was performed. The first activity performed involved analysis of the detailed system documentation to determine if and how the security requirements were met. When necessary, additional documentation was developed. Other major activities included performing system testing (see Section 3) and conducting a risk analysis. The analysis established the extent that the KES met the security requirements defined.

A risk analysis group was formed by NSA to assess the appropriateness of the safeguards to minimize risk, while the security testing focused on the functionality and effectiveness of the safeguards.

Step 4 - Report Findings and Recommendations

This step involved documenting and coordinating the results of Step 3, and preparing a recommendation and certification package. The certification package contains a set of supporting documentation including: test results, risk assessment, and the KES P&P. The KECWG also provided a recommendation and statement of residual risk to the Accreditor. The purpose of this total package was to assist the Accreditor in approving the system for operation.

3.0 System Testing

The testing of the Interim KES was a required step in the C&A of the system. DOJ served as the system accreditor for the Interim KES and was charged with ensuring that the system was adequately tested prior to accreditation. The KECWG was formed to assist DOJ with the accreditation of the system by developing test plans, providing organization for the tests, and serving as the test coordinator.

3.1 Test Organization

The system tests were divided into two phases: a walk through of KES P&P and the official test. The walk through differed from the official test in several important aspects. The walk through followed the P&P to ensure that all procedures for each subsystem were adequately documented. However, the procedures were not necessarily performed sequentially. During the walk through,

all tests involving the extraction and release of keys utilized test keying materials. Also, no oversight by the system accreditor was required for the walk through. The C&A contractor was present during the walk through to provide organization and to note corrections to the P&P and the draft test plan. An additional benefit of the walk through was to familiarize the staff with the various pieces of KES equipment and procedures prior to the official test. The walk through took place during May 1995.

The official test was divided into the testing of each of the KES subsystems following the documented procedures of the P&P. The test was not considered "end to end" because no single chip was not tracked throughout the entire process (programming through release), and the tests did not necessarily follow a sequential format. The testing of the extraction and release of encrypted Key Components (KC) did follow a chronological format and was conducted "end to end" during the course of one day. The tests were observed by the system accreditor (or representative) and one independent observer at each subsystem site. The testing of the programming site occurred during the June 5, 1995 programming session at Mykotronx in Torrance, CA. The official test of the encrypted KC release was performed on November 4, 1995.

All results and observations were reviewed by the KECWG and included in the accreditation package, which was sent to DOJ. Recommendations for changing procedures resulting from the walk through and the official test were handled through the KES configuration management process. Though the official test was a comprehensive "positive test" utilizing the best case scenario, all procedures were thoroughly tested and all agencies participated.

3.2 Programming Site Testing

Certification testing was conducted during a regular chip programming session at the programming site in Torrance CA. Chip programming was conducted over a period of one week. All testing associated with programming was supervised by a certifying official and an independent observer. The test was positive, with no errors intentionally inserted. However, participants were asked to document appropriate areas for future negative testing. Testing included physical security procedures, programming device initialization, key component generation, chip programming, software archiving, system sanitization, and key component transportation. Test logs were based on the KES P&P, and followed a chronological format. Modifications to the P&P were noted for inclusion in the next release of the P&P document.

Preparatory work for the programming session was also tested and documented at each Escrow Site. This included physical security, computer initialization, development of programming seed materials, and transportation of the seed materials to the programming site. Upon return to the Escrow Sites, the key component storage procedures were also tested and documented.

3.3 Extraction and Release Testing

Certification testing of the key component release occurred during regular working hours at NIST, Treasury, DOJ, and the FBI. The test was conducted during the course of a single day.

Actual extractions and releases may be required during off hours; however this test was set up to simulate the most ideal scenario. Timing information was collected during the official test. This information was not used to accredit the timing for the extraction and release, but was used to estimate the time required for each process. No errors were intentionally introduced during this test, but the teams of evaluators and test participants were instructed to note areas where appropriate error testing could be incorporated. The test coordinator maintained contact with each of the teams by phone during the test and attended the test of the decryption process. In order for the test to be conducted simultaneously at all subsystem sites, three teams of observers were formed. Each team had two members: one representing the system accreditor and one serving as independent observer.

The test of the extraction process utilized key components for AT&T Telephone Security Device Model 3600 (Clipper Chip based phones) owned and retained by the FBI. The Authorization for the release of key components for these devices for testing purposes, was granted by the United States Attorney General on August 23, 1995, in a memorandum to the Director of the FBI, Louis Freeh. The authority for the intercept was granted for a period of one month and was discontinued upon the completion of testing. The discontinuation of the intercept prior to the end of the deadline is consistent with the guidelines set forth by the United States' Attorney General.

The FBI provided both the facility and equipment for the intercept and decryption of the communications. The process utilized the internal phone system at the FBI facility and two FBI owned AT&T TSD3600s . A representative from DOJ, one independent observer, two Escrow Officers, and two FBI agents were required during the test of the decryption process. The Escrow Officers providing the extraction diskettes witnessed the decryption process; though this would not be allowed during an actual intercept situation.

4.0 SUMMARY

In order to be successful, a multi-agency certification of a National system requires coordination, planning, and established structure. The following actions are essential to the success of the C&A effort.

1. Establishing a charter enabled the KECWG to define the purpose of the group, establish the group's organization, outline required activities, and define the decision making process.

2. Ensuring that the KECWG members from the federal agencies were fully authorized to represent their agency, allowed critical decision making during the meetings.

3. Defining the security requirements early in the system life cycle provided a solid basis for testing, and ensured system security at each test point.

4. Developing the residual risk statement in a group setting provided the membership and

the accrediting authority with a full understanding of the risk analysis.

5. Having the accrediting authority actively involved from the beginning of the certification process provided an assurance of final accreditation.

There were two areas that were not as effective and should have been performed differently. First, the risk analysis was performed independently by an outside group without shadowing by the certification working group. Since the analysis was accomplished without the participation of the KECWG, modifications to the system and procedures could not be dynamically introduced into the process. Thus, the analysis required an update upon its first review by the KECWG. Second, the chair of the KECWG should have had more authority to enforce deadlines and scheduling. The enforcement of deadlines was made more complex by the interagency nature of the project.

At the writing of this paper, all certification activities have been completed and the certification package is being compiled. Once complete, the certification package will be sent to DOJ for approval and system accreditation. The completed activities have been very successful and the certification process has yielded several unexpected benefits. Certification testing identified areas in the P&P where additional granularity was required. It also pointed out areas where procedures could be optimized. The test results and comments from the testers were folded into the current P&P baseline. In addition, the System Test and Evaluation Plan will form the basis for the overall KES Test Plan. The KES Test Plan will be used for both system testing and training for the Escrow Officers. The development of the statement of residual risk provided an open forum for the discussion of both the physical and technical security of the system. These discussions provided the KECWG with additional assurance of the security of the system.

REFERENCES

National Institute of Standards and Technology, "Federal Information Processing Standards Publication 185, Escrowed Encryption Standard", 4 February 1994.

National Institute of Standards and Technology, "Federal Information Processing Standards Publication 102, Guideline for Computer Security Certification and Accreditation", 27 September 1983.

National Security Agency, "Certification and Accreditation Process Handbook (Draft)", NCSC-TG-031, February 1994.

Office of Management and Budget, "Circular No. A-130, Management of Federal Information Resources", 12 December, 1985.